UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,649	12/30/2003	Ju-Han Kim	51876P550	7916

8791 7590 04/30/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
YOUNG, NICOLE M	
ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
04/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/749,649	KIM ET AL.	
	Examiner	Art Unit	
	Nicole M. Young	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 December 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 12/30/2003
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The Applicant uses the language "means for" throughout the claim language. The Examiner does not consider 112 6th paragraph invoked as there is a structure (XML) within the claim language.

Drawings

The drawings are objected to under 37 CFR 1.83(a) because they fail to show information management system 13 as described in the specification (for example, page 10 line 19). Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-10 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1 refers to, "an integrated security information management system". The system of the claim has no structure. Generally, functional descriptive material, such as a computer program, is statutory when it is stored on a tangible computer readable medium. See MPEP § 2106 IV.B.I(a). Claims 2-5 are depended on claim 1 and do not provide further structure, therefore they are non-statutory as well. Claims 1-5 also have no useful result.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 and 6 recite the limitation "the integrated security information management client". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Cross et at. (US 2004/0162786) herein referred to as Cross.

Claim 1 discloses an integrated security information management system , comprising:

an Extensible Markup Language (XML) key managing (figure 7 XKMS Client 776 and associated text) means for performing an interface with an external security information management client based on an XML, authenticating a user, analyzing a request from the integrated security information management client, and requesting a processing to an access control means (Logon Screen 760 and associated text), an authenticating means or an external public key infrastructure certification server (figure 6, key pair 608 and associated text) depending on a request kind (Fig. 6 and 7 and associated text where the Digital Identification Management Service is interpreted to be the integrated security information management system);

the access control means for providing a user authenticating function (Logon Screen 760 and associated text, also paragraph [0025]), an access authority policy generating function for limited shared data storing means (paragraph [0025], "authentication...digital ID's"), an access authority confirming function depending on the access authority policy (paragraph [0025], "authentication...digital ID's"), a shared security information providing function for an access-allowed user (paragraph [0025] where in "authentication...digital ID's" shares security information), a security information position information providing function (paragraph [0025] wherein

"authentication...digital ID's" provides security information), a shared security information registering/deleting/updating function (paragraphs [0025] and [0044] wherein "The DIMS...IDs" includes "storing, retrieving, deleting, listing (enumerating) and verifying digital ID's), a shared security information share setting/releasing function (paragraphs [0025], [0044], and [0052] wherein the shared security information setting function refers to "with proper permissions set"), and an XML digital signature / verification / encryption / decryption / communication security function depending on a shared security information processing request from the XML key managing means (Fig. 6 and 7 and associated text, especially 609 and 776);

the authenticating means for providing the user authenticating function (paragraph [0025], "authentication...digital ID's"), a person-in-question authenticating function (paragraph [0025] where credential management is interpreted to be person-in-question]), a non-shared security information providing function for the access-allowed user (the person-in-question) (paragraph [0052] where permissions are interpreted to be information providing function), a security information position providing function (paragraph [0025] where "authentication...digital ID's" provides position information), a non-shared security information registering / modifying / deleting function (paragraph [0053] where the personal store is not shared), and the XML digital signature/ verification / encryption / decryption / communication security function depending on a non-shared security information processing request from the XML key managing means (paragraph [0070] "XML Key Management...trust information");

the limited shared data storing means for storing and managing security information shared by an object limited depending on a control of the access control means (paragraph [0052] pertaining to permissions); and

non-shared data storing means for storing and managing security information that should not be shared depending on control of the authenticating means (paragraph [0053] where My Store is not scared, also "while any digital ID...user's messages").

Claim 2 discloses the integrated security information management system as recited in claim 1, wherein in the access authority confirming function depending on an access authority policy of the access control means, if the access control means receives an access request to the limited shared data storing means from the XML key managing means, after a user authentication is performed, the access authority policy corresponding to the requested security information is read to confirm whether or not a user has authority (Fig. 6 and 7 and paragraph [0025]).

Claim 3 discloses the integrated security information management system as recited in claim 2, wherein when the user registers the security information through the integrated security information management client, the access authority policy is generated and is continuously and dynamically updated depending on updating/deleting and share setting/releasing of the security information later registered (paragraphs [0053] and [0054]).

Claim 4 discloses the integrated security information management system as recited in any one of claims 1 to 3, wherein the access control means and the authenticating means uses a signature received from a security information owner according to the request of the integrated security information management client to further perform a

security information share-agency setting function for allowing other users to set/release a share and a function of informing the security information owner of a security information share-agency setting request (paragraph [0046]).

Claim 5 discloses the integrated security information management system as recited in claim 4, wherein the access control means and the authenticating means uses a signature and a certificate issued from other users according to the request of the integrated security information management client to further perform a shared security information retrieving function for retrieving the security information shared by a self, a shared security information retrieval confirming function for informing the security information owner of execution of the shared security information retrieving function depending on the execution, and a shared security information usage log confirming function for confirming a log for a shared security information usage (paragraphs [0046] and [0071] and [0072] which describe an enterprise trust model with multiple clients).

Claim 6 discloses an integrated security information management method, comprising the steps of:

classifying security information depending on its kind according to a security information registering / updating / deleting request from an integrated security information management client to register/update/delete the classified security information from a limited shared data storage or a non-shared data storage at an integrated security information management system (paragraphs [0044] "The DIMS...digital ID's" and [0088] pertaining to renewing digital ID's and life cycle functions);

setting/releasing a share for the security information registered into the limited shared data storage according to a security information share setting/releasing request from the integrated security information management client, and generating/updating a security access authority policy at the integrated security information management system (paragraphs [0053] and [0054], ""the user can...management tasks");

confirming a request user's authority depending on a security access authority policy according to a shared security information providing request from the integrated security information management client, and then providing corresponding security information for the integrated security information management client at the integrated security information management system (Fig. 6 and 7 and paragraph [0025], where in "authentication...digital ID's" confirms and provides security);

authenticating that a request user is a non-shared security information owner according to a non-shared security information providing request from the integrated security information management client, and then providing corresponding security information for the integrated security information management client at the integrated security information management system (Fig. 6 and 7 and paragraph [0025]m where in "authentication...digital ID's" authenticates and provides); and

generating/verifying a digital signature according to a digital signature generating/verifying request using an XML from the integrated security information management client at the integrated security information management system (Fig. 6 and 7 and paragraphs [0025] and [0046] "use in authentication, digital signature, encryption/decryption processes").

Claim 7 discloses the integrated security information management method as recited in claim 6, further comprising the step of:

informing a security information owner of a security information share-agency setting request according to an other owners' security information share-agency setting request from the integrated security information management client to receive acknowledgement, and then allowing other users to use a signature received from the security information owner to set/release the share for corresponding security information at the integrated security information management system (paragraphs [0046] and [0071] and [0072] which describe an enterprise trust model with multiple clients).

Claim 8 discloses the integrated security information management method as recited in claim 6 or 7, further comprising the step of:

informing the security information owner of a security information verifying request according to an other owners' security information verifying request from the integrated security information management client to receive acknowledgement, and then providing a verified result of other owners' security information for the integrated security information client at the integrated security information system (paragraphs [0046] and [0071] and [0072] which describe an enterprise trust model with multiple clients).

Claim 9 discloses the integrated security information management method as recited in claim 8, wherein the security information registering / updating / deleting step comprises the steps of:

a user's requesting an extensible XKMS server of the integrated security information management system for security information registration / update / deletion through the integrated security information management client;

authenticating the request user and confirming a security information kind at the extensible XKMS server;

as the confirmation result, if the security information kind is sharable, sending the request to an access control server to register / update / delete the security information from-a limited shared data storage; and

as the confirmation result, if the security information kind is non-sharable, sending the request to an authentication server to register / update / delete the security information from a non-shared data storage (Figures 6 and 7 and associated text, particularly paragraphs [0124]-[0127] which explain XKMS Client 776 and how it interacts with the life cycle manager).

Claim 10 discloses the integrated security information management method as recited in claim 8, wherein the security information share setting/releasing step comprises the steps of:

a user's requesting the extensible XKMS server of the integrated security information management system for security information share set/release through the integrated security information management client;

authenticating the request user at the extensible XKMS server, and then sending a security information share setting/releasing request to the access control server, and

loading an access authority policy for corresponding security information at the access control server, and then confirming whether or not the access authority policy is set to allow the request user to share; and

as the confirmation result, in case the access authority policy is set to allow the request user to share, reading the corresponding security information from the limited shared data storage to send the read security information to the request user through the integrated security information management client (Figures 6 and 7 and associated text, particularly paragraphs [0124]-[0127] which explain XKMS Client 776 and how it interacts with the life cycle manager).

Note: Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-270-1382. The examiner can normally be reached on Monday through Friday, alt Fri off, 8:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY

Tariq T. Arani
Primary Examiner
T. Arani
4/25/07